CAUCHY: Jurnal Matematika Murni dan Aplikasi
Volume 10(1) (2025), Pages 374-388
p-ISSN: 2086-0382; e-ISSN: 2477-3344

Logistic Map with Feedback Control for Resilient Image Encryption

Mohammad Fahrurrozy*, Agus Suryanto, Isnani Darti

Department of Mathematics, Faculty of Mathematics and Natural Sciences,
University of Brawijaya, Indonesia

Email: mohfahrurrozy@student.ub.ac.id

ABSTRACT

Images are widely used to store and share important information due to their ease of use and accessibility. However, they are also vulnerable to cyber-attacks. An encryption effort is needed to secure the vital information in an image. In this paper, an encryption and decryption algorithm for grayscale and RGB images is proposed using logistic map with feedback control (LMFC). This 2D map which is an improvement from the popular one-dimensional logistic map also exhibits sensitive dependence on initial conditions, known as chaos. This phenomenon is verified through bifurcation diagram and the largest Lyapunov exponent. By using the largest Lyapunov exponent and the control parameters as secret key, LMFC generates two sequences of pseudo-random number related to the original image. Subsequently, a permutation process is proposed, utilizing permutation box to rearrange the pixel positions in the plain image. Finally, a diffusion process is proposed, utilizing XOR operations and keystreams created from the pseudo-random sequence to alter the pixel values, resulting in a visually distinct cipher image. Performance analysis of the proposed algorithm indicates resilience to various cryptanalysis and robust security, as it is sensitive to both secret keys and plain image. Additionally, the proposed decryption algorithm demonstrates the ability to reconstruct the original image with good quality from a cipher image, despite data changes or losses.

Keywords: Cybersecurity, Image encryption, Chaotic cryptography, Pseudo-random sequence, Lyapunov exponent

INTRODUCTION

In today's digital era, every aspect of human life depends on information. With vast amounts of information being stored and shared digitally, ensuring its security and privacy is essential. Images are among the most commonly used forms of information and often contain sensitive content, requiring secure protection [1]. Therefore, robust encryption techniques using cryptography are necessary to secure image data from unauthorized access and cyber threats.

Cryptography has become a crucial field in ensuring the security of information, as it involves the study of data encryption techniques. The two main concept of cryptography

Submitted: December 16, 2024 Reviewed: February 26, 2025 Accepted: May 06, 2025
DOI: https://doi.org/10.18860/cauchy.v10i1.30783

are encryption and decryption. The process of encoding an information (plaintext) into an encoded message (ciphertext) is called encryption. Meanwhile, the process of reversing the ciphertext back into plaintext is called decryption. According to Shannon [2], a secure communication needs two crucial concepts, that is confusion and diffusion. Confusion is about complex relationship between plaintext and the secret key so that there is no obvious pattern. Diffusion suggests that information spread throughout the entire ciphertext, resulting in a huge difference to ciphertext whenever there is a slight difference in the plaintext. One of the most popular encryption algorithms that used the confusion and diffusion concept is Advanced Encryption Standard (AES) which utilized by plenty of researchers in image encryption [3]. However, AES is not well-suited for image encryption due to the inherent characteristics of images, including large size, high redundancy, and strong correlations among adjacent pixels [4].

Chaos theory is one of many mathematical fields that have a big impact on the concept of confusion and diffusion. Chaos theory studies chaotic dynamical systems which have plenty of advantages in communication security, such as sensitive to initial condition, noise-like behavior and easy to produce a pseudo-random sequence. One of the most popular dynamical systems is the logistic model. Over the years, the logistic model is being studied and developed, such as adding the feedback control variable and becomes the logistic model with feedback control [5]. In 2015, the model is discretized using the forward Euler method and becomes the logistic map with feedback control [6]. Furthermore, bifurcation analysis shows that the logistic map with feedback control undergoes flip bifurcation. Hence, the map is chaotic.

It is not uncommon nowadays for chaotic dynamical systems being used in image encryption, such as the continuous-time dynamical systems [7-11] and discrete-time dynamical systems [12-18]. Not only that, some researchers also introduced their own new dynamical systems which exhibits chaotic behavior more than the common ones to maximize the encryption quality [12-14]. However, some research that applied the common dynamical systems for image encryption also have good results. Demirtaş [19] presented an algorithm based on Henon map and 3D bit-scrambling to encrypt multiple images. With the help of the chaotic Henon map to generate the pseudo-random sequence, the method passes performance analysis and robust against different cryptanalytic attacks. Akraam et al. [20] presented a scheme of image encryption that combines several chaotic maps. They utilized four of the most popular discrete-time maps, such as tent map, piecewise linear chaotic map, logistic map and Henon map. The combined chaotic maps successfully created a keystream to diffuse the pixels value. This proposed encryption method is resilient against well-known attacks. Arif et al. [21] have presented a novel image encryption method with logistic map as a base. The encryption process uses the permutation and substitution method using S-box to obtain the cipher image which exhibits very high sensitivity concerning plain image and secret key. De et al. [22] in his algorithm used three different chaotic maps, such as Chebyshev map, logistic map and Beddington, Free and Lawton (BFL) map. The keystream created by the XORing the generated pseudo-random sequence from the three different maps passed the NIST randomness test. The proposed scheme achieves a significant improvement from the compared method in terms of sensitivity and correlation coefficient.

Based on the background and findings from various studies, it can be determined that logistic map and the other common chaotic maps can become the foundation of a sensitive, robust, and competitive encryption algorithm. Therefore, this paper aims to apply the logistic map with feedback control that has been studied in [6] to an image encryption algorithm. The presented algorithm is employed to produce a secure cipher

image, while also capable of producing a robust decrypted image.

METHODS

Largest Lyapunov Exponent

The Lyapunov exponent characterizes the rate of separation (or attraction) of orbits that very close to a fixed point of a map. When a map is sensitive to initial conditions, its close orbits diverge exponentially. This separation of orbits implies positive average exponential rates. Therefore, the positive Lyapunov exponent serves as an indicator for the emergence of chaos. Consider the map

$$\vec{x}_{n+1} = f(\vec{x}_n), n \in \mathbb{Z} \vee n \in \mathbb{N}, \vec{x} \in \mathbb{R}^k. \quad (1)$$

where $\vec{x} = (x_1, x_2, \dots, x_k)^T$ and $f: \mathbb{R}^k \to \mathbb{R}^k$. Suppose $\vec{y}_0$ and $\vec{y}_n$ is the perturbations of $\vec{x}_0$ and $\vec{x}_n$, respectively, where $\vec{x}_0 = (x_{10}, x_{20}, \dots, x_{k0})^T$ is the initial value of the map (1) and $\vec{x}_n = (x_{1n}, x_{2n}, \dots, x_{kn})^T$ is the value at iteration n in the map (1). The perturbation $\vec{y}_0$ evolves exponentially over time to become $\vec{y}_n$. By linearizing the map (1), the perturbation $\vec{y}_n$ can be expressed as

$$\vec{y}_n = \prod_{i=0}^{n-1} \left(\mathcal{D}f(\vec{x}_n)\right) \vec{y}_0 .$$

The Lyapunov exponent can be formulated as

$$\lambda_k = \lim_{n\to\infty} \frac{1}{n} \ln \frac{\|\vec{y}_n\|}{\|\vec{y}_0\|}.$$

In order to avoid the huge calculation of $\|\vec{y}_n\|$ as $n \to \infty$, one can normalize $\vec{y}_n$ first. Consider the unit vector $\vec{y}_0$. For $i = 1,2, \dots, n$, vector $\vec{y}_i$ can be normalized as

$$\vec{y}_i = \frac{\boldsymbol{y_i}}{\|\boldsymbol{y_i}\|},$$

where $\boldsymbol{y_i} = \left(\mathcal{D}f(\vec{x}_{i-1})\right)\vec{y}_{i-1}$ and $\mathcal{D}f(\vec{x}_i)$ is the Jacobian matrix of map (1). The largest Lyapunov exponent can be computed as [23]

$$\lambda_{\max} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln\|\boldsymbol{y_i}\| ,$$

or can be approximated as

$$\lambda_{\max} \approx \frac{1}{\mathcal{N}} \sum_{i=1}^{\mathcal{N}} \ln\|\boldsymbol{y_i}\| , \quad (2)$$

for some large number $\mathcal{N}$. If $\lambda_{\max} > 0$, then map (1) is chaotic.

Logistic Map with Feedback Control

The logistic map is a widely recognized discrete dynamical system that undergoes bifurcation, marked by drastic shifts in its behavior when there is a slight change in its parameter. The logistic map is denoted by

$$x_{n+1} = r x_n (1 - x_n), \quad (6)$$

where the variable state is denoted by $x_i \in [0,1]$ and the control parameter is represented by $r \in [0,4]$. The bifurcation diagram and the largest Lyapunov exponent of map (6) is shown in Figure 1.

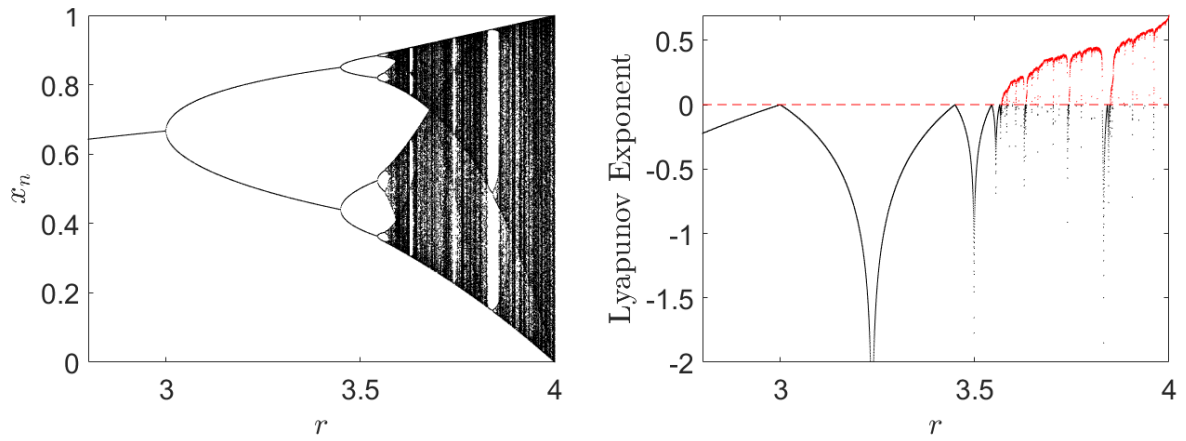

Figure 1. Bifurcation diagram and largest Lyapunov exponent graph of logistic map

In 1992, Gopalsamy and Weng [5] introduced a new model incorporating the logistic equation with feedback control, expressed as follows

$$\begin{aligned} \frac{dx}{dt} &= rx\left(1-\frac{x}{k}-cu\right), \\ \frac{du}{dt} &= -bu+ax, \end{aligned} \tag{7}$$

where x represents the population density, u is the variable of feedback control and r is the intrinsic growth rate. Aditionally, a, b, and c are positive parameters, and k denotes the carrying capacity of the population. In 2015, Wu [6] applied the forward Euler method to model (7) to get the following logistic map with feedback control (LMFC) as

$$\begin{aligned} x_{n+1} &= x_n + \delta[rx_n(1-x_n) - cx_nu_n], \\ u_{n+1} &= u_n + \delta[-bu_n + ax_n], \end{aligned} \tag{8}$$

where δ is the step size. In order to show that LMFC is undergoes period-doubling bifurcation and chaos, we give the bifurcation diagram of LMFC and the largest Lyapunov exponent graph in Figure 2 using initial condition $(x_0, u_0) = (0.6, 0.4)$, control parameter $(r, a, b, c) = (1.9, 0.01, 0.1, 0.4)$, $\mathcal{N} = 5000$, and stepsize $\Delta_\delta = 0.0001$.

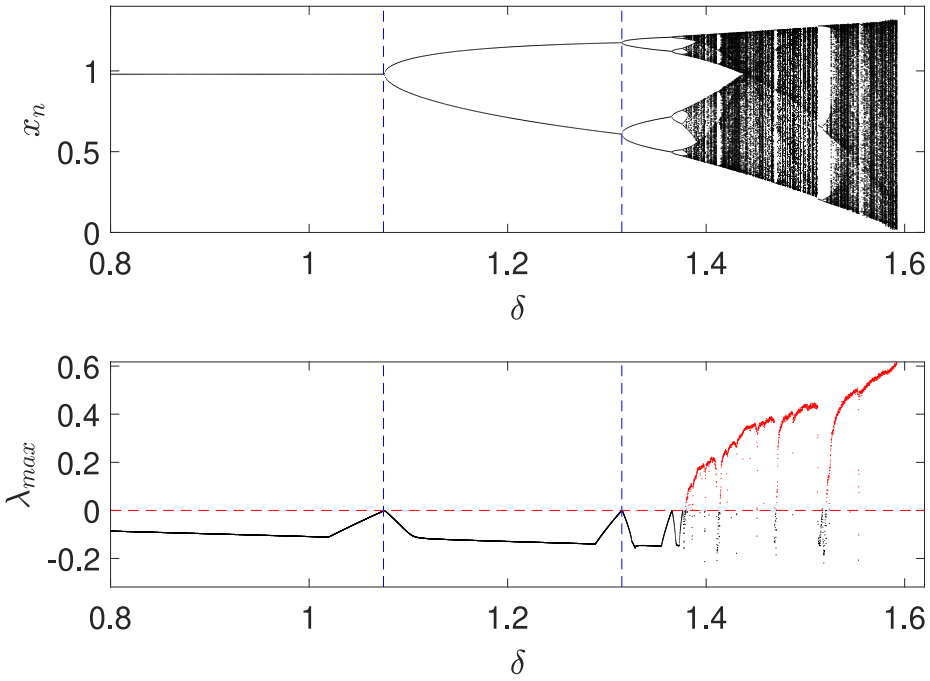

Figure 2. Bifurcation diagram and graph of largest Lyapunov exponent of LMFC

Figure 2 indicates that LMFC undergoes period-doubling bifurcation. Based on the positive largest Lyapunov exponent of LMFC, it can be concluded that LMFC is chaotic or sensitive to initial conditions. Furthermore, LMFC is chosen over other chaotic maps because it is a two-dimensional chaotic system that generates two random sequences simultaneously, unlike the commonly used logistic map in image encryption. These two sequences would be beneficial in creating a complex encryption algorithm.

The crucial aspect to generate random sequences with LMFC is the parameter values. From Figure 2, one can observe that the positive largest Lyapunov exponent is increasing for $1.55 \leq \delta \leq 1.5972$, but have no value as $\delta > 1.5972$. This implies that there is some $\delta \in [1.55,1.5972]$ where $\lambda_{\max}$ has the maximum value which causes the level of chaos of LMFC is at the highest point. The most pseudo-random sequences, x_n and u_n, can be produced from LMFC using this matching δ value. However, if $\lambda_{\max} < 0$, then the δ value cannot be used to generate the pseudo-random sequence because the negativity of $\lambda_{\max}$ indicates that LMFC is not chaotic.

Proposed Encryption Algorithm

Encryption algorithm started with obtaining the δ value which maximizes the largest Lyapunov exponent of LMFC. Then, permutation and diffusion process are introduced to shuffle the pixel positions and alter the pixels value, respectively, to add the confusion-diffusion concept in the algorithm.

Let P be a grayscale image of $M \times N$ size, where M and N is the number of rows and columns of P, respectively, while the i-th pixel of P is denoted by P_i. Let the control parameter of LMFC, that is r, a, b, c as the secret keys, while the initial condition of LMFC is $(x_0, u_0) = (0.6, 0.4)$.

Step 1: Compute the sum of pixels of P as

$$S = \sum_{i=1}^{M \times N} P_i.$$

Step 2: The new secret key value is obtained as

$$r' = r + \mathrm{mod}\left(\frac{S}{M \times N \times 255}, 1\right) \times 10^{-3}, \qquad a' = a + \mathrm{mod}\left(\frac{S}{M \times N \times 255}, 1\right) \times 10^{-3},$$

$$b' = b + \mathrm{mod}\left(\frac{S}{M \times N \times 255}, 1\right) \times 10^{-3}, \qquad c' = c + \mathrm{mod}\left(\frac{S}{M \times N \times 255}, 1\right) \times 10^{-3}.$$

Step 3: Compute the largest Lyapunov exponent of map in LMFC using Equation (5), where

$$\mathcal{D}f(x,u) = \begin{pmatrix} 1 + \delta r' - 2\delta r' x - c\delta u & -c'\delta x \\ a'\delta & 1 - b'\delta \end{pmatrix},$$

is the Jacobian matrix of LMFC, $\mathcal{N} = 500$ with step size 0.0005. The δ value which maximizes the largest Lyapunov exponent is chosen for further encryption process. The secret keys r', a', b', c' and δ are obtained before the encryption process. Thus, the secret keys can be shared through a secret channel to be used in the decryption process.

The second process is the permutation process. This process shuffles the pixel positions in order to acquire the scrambled image P'.

Step 1: Iterate LMFC using control parameter r', a', b', c', δ and initial condition $(x_0, u_0) = (0.6, 0.4)$ to get a pseudo-random sequence X and U.

Step 2: Obtain the new sequence Z by multiplicating X and U and sort it in ascending order to acquire sort(Z).

Step 3: Permute the indices of P with the indices of sort(Z) and obtain P' as the shuffled sequence of pixels of P.

The last process of the encryption method is the diffusion process, which alters the

pixel values of P' to obscure the image's pixel information using the bit-wise XOR operation.

Step 1: Generate the keystreams K_1 and K_2 based on X and U as follows.

$$K_1 = \text{mod}\ (\lfloor X \times 10^{10} \rfloor, 256),$$
$$K_2 = \text{mod}\ (\lfloor U \times 10^{10} \rfloor, 256).$$

Step 2: Execute the bit-wise XOR operation between P_i' and K_{1i} consecutively from $i = M \times N$ to $i = 1$ to obtain the sequence C', i.e.,

$$C_i' = \begin{cases} P_i' \oplus K_{1i} & , \quad \text{if } i = M \times N \\ (P_i' \oplus K_{1i}) \oplus C_{i-1}', & \quad \text{if } i \neq M \times N \end{cases}$$

Step 3: Execute the bit-wise XOR operation between C_i' and K_{2i} consecutively from $i = M \times N$ to $i = 1$ to obtain the sequence C^*, i.e.,

$$C_i^* = \begin{cases} C_i' \oplus K_i & , \quad \text{if } i = M \times N \\ (C_i' \oplus K_i) \oplus C_{i-1}^*, & \quad \text{if } i \neq M \times N \end{cases}$$

Step 4: The sequence C^* is transformed into a matrix of size $M \times N$ to obtain the cipher image C.

For RGB images, the encryption process can be done by separating the color image into three grayscale images from the red, green, and blue channels. After that, the encryption process is performed individually on these three images, which are then combined back into one color image at the end of the encryption process, with the exception that the value of S in step 2 of permutation process is one-third of the sum of all pixels in each red, green, and blue channel.

Decryption Algorithm

The decryption algorithm requires the secret keys r', a', b', c' and δ that have been shared from secret channel and cipher image C as the input. The method is the opposite of the encryption algorithm without obtaining the δ value.

Data

We obtained the images used in this paper from the USC-SIPI dataset. They are composed of four grayscale images with dimensions of 256×256 (cameraman.tif, clock.tif), 512×512 (boats512x512.tif, and baboon_gray.tif), and four RGB images with dimensions of 256×256 (peppers.png, house.tif), and 512×512 (baboon.tif, airplane.tif). All of the images used can be seen in Figure 3 and Figure 4. After encrypted into cipher images, all of the grayscale images will be used to evaluate the performance of the proposed encryption and decryption algorithm through several methods, namely: correlation analysis, plain image sensitivity analysis, key sensitivity analysis, histogram analysis, Mean Square Error (MSE) and Peak Signal-to-Noise Ratio Analysis (PSNR), entropy analysis, and robustness analysis.

RESULTS AND DISCUSSION

The encryption and decryption procedures were conducted utilizing MATLAB 2014b on an individual computer featuring an Intel Celeron N4020 CPU 1.10GHz with 4 GB of RAM. Secret keys $(r, a, b, c) = (1.9, 0.01, 0.1, 0.4)$ are used. Figure 3 and Figure 4 shows the encrypted grayscale and RGB images with size 256×256 and 512×512 give entirely no resemblance to the plain images. Meanwhile, the decrypted grayscale and RGB images are purely identical with the plain images.

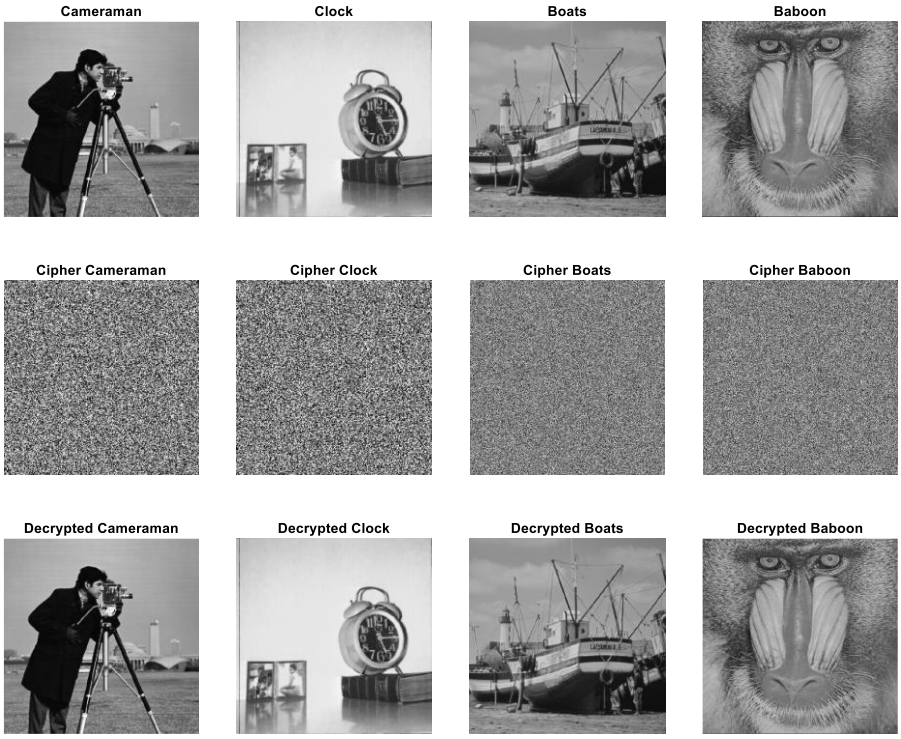

Figure 3. Encryption and decryption result of grayscale images

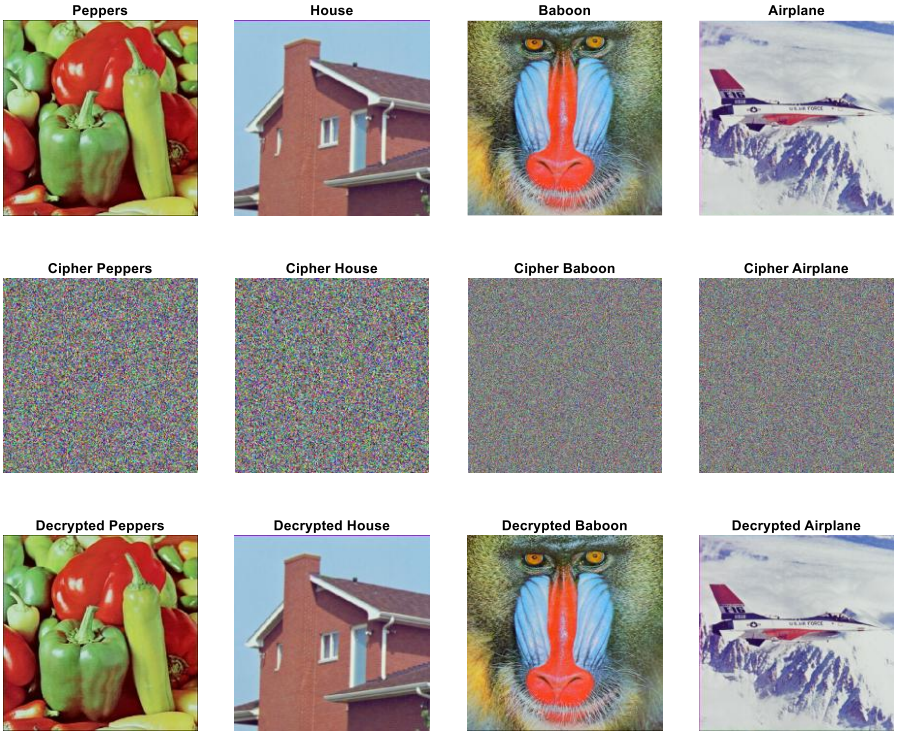

Figure 4. Encryption and decryption result of RGB images

Key Space Analysis

The set of all possible values of the secret key is called key space. The number of possible keys determined the key space size. With the intention to withstand a brute-force attack, a key space larger than 2^{128} is suffice [24]. For the proposed algorithm, assuming the computing precision is 10^{-15} for each key r, a, b, c, then the key space has a magnitude of $(10^{15})^4 \approx 2^{199} \gg 2^{128}$. As a result, the size of the key space ensures protection against brute-force attacks.

Correlation Analysis

The presence of a strong correlation between adjacent pixels results in an image rich in information. A cipher image is expected to demonstrate a low correlation among its adjacent pixel values. Correlation coefficient is a quantitative measure to determine the correlation in an image. Correlation coefficient can be described as follows [25]

$$CC_{\kappa\iota} = \frac{\sum_{i=1}^{N}\left(\kappa_i - E(\kappa)\right)\left(\iota_i - E(\iota)\right)}{\sqrt{\sum_{i=1}^{N}\left(\kappa_i - E(\kappa)\right)^2 \sum_{i=1}^{N}\left(\iota_i - E(\iota)\right)^2}},$$

where κ and ι are the pixel values of two adjacent pixels, while $E(\cdot)$ is the average of the selected pixels.

A secure encryption algorithm ought to eliminate the strong correlation from the plain image which becomes a cipher image with a weak correlation or no correlation among its adjacent pixels. The correlation of the image is weak if the correlation coefficient is nearly 0. With the goal to calculate the correlation coefficient of the image, we randomly choose 3000 pixels and its adjacent pixel in each direction. Then, we create the scatter diagram of the chosen pixels and its adjacent pixels to show the distribution of the pixels. Also, we calculated the correlation coefficient to show that there is no correlation in the cipher image.

Figure 5 illustrated the distribution of the chosen adjacent pixels in each direction for grayscale image Cameraman. As we can see, the plain image pixels are dominant in the diagonal, while the cipher image pixels distributed uniformly. The correlation coefficients of cipher grayscale images are given in Table 1. One can observe that the correlation coefficient values of cipher images are nearly 0. This shows that the algorithm strongly removes the strong correlation of the plain and cipher images have almost no correlation among its adjacent pixels. Also, compared with other literatures in Table 2, our method has certain advantages.

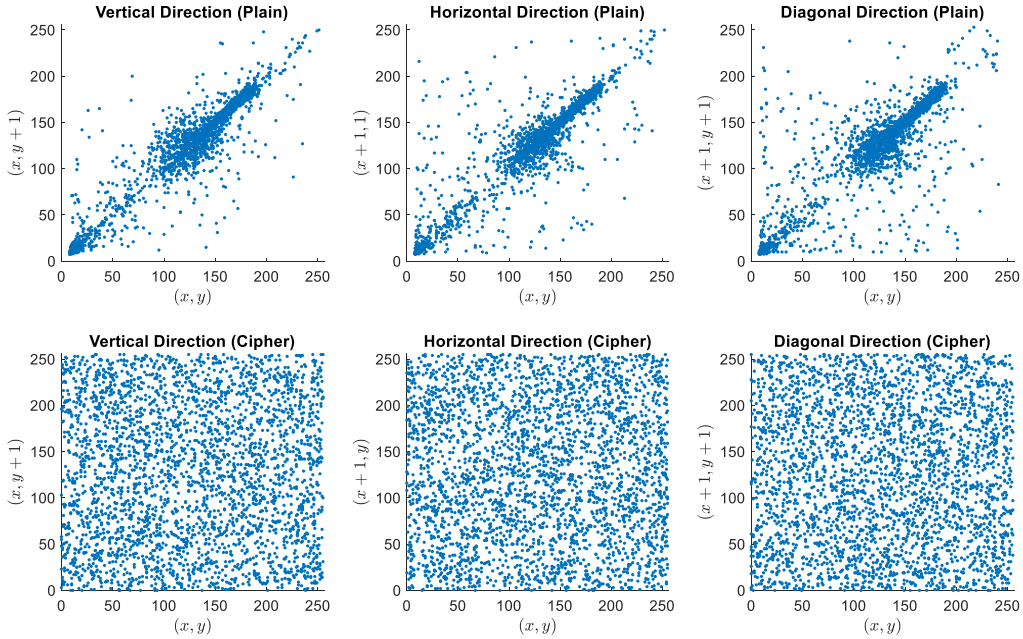

Figure 5. Scatter diagram of the chosen neighbouring pixels of plain image and cipher image Cameraman in 3 different directions

Table 1. Correlation coefficients of grayscale images

Grayscale Cipher Image	Correlation Coefficient		
	Horizontal	**Vertical**	**Diagonal**
Cameraman	0.00884	0.00054	-0.00382
Clock	0.00328	0.03467	0.00942
Boats	-0.02602	0.00792	0.00348
Baboon	-0.00650	-0.00859	-0.01148

Table 2. Correlation coefficient of Cameraman image compared with other methods

Method	Correlation Coefficient		
	Horizontal	**Vertical**	**Diagonal**
Proposed	0.00884	0.00054	-0.00382
[19]	-0.00186	-0.00485	-0.00624
[21]	0.00235	0.03449	-0.00559

Plain Image Sensitivity Analysis

A strong encryption algorithm must exhibit sensitivity to the plain image. There are two metrics that can be used to evaluate the sensitivity of the plain image, that is the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) which can be described as the equation

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} K(i,j) \times 100\%,$$

and

$$\text{UACI} = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|CI_1(i,j) - CI_2(i,j)|}{M \times N \times 255} \times 100\%,$$

where $CI_1(i,j)$ and $CI_2(i,j)$ are two cipher images as a result from two plain image with one-pixel difference and

$$K(i,j) = \begin{cases} 1, & \text{if } CI_1(i,j) \neq CI_2(i,j) \\ 0, & \text{if } CI_1(i,j) = CI_2(i,j) \end{cases}.$$

The optimal NPCR and UACI values are approximately 99.6% and 33.46%, respectively [26]. In order to calculate the UACI and NPCR value, we created the one-pixel difference image from the grayscale plain images in Figure 4 and encrypted them. Table 3 displays the NPCR and UACI measurements for grayscale images. The result indicates that the UACI and NPCR values are within close range of the optimal values. Hence, the proposed algorithm exhibits sensitivity to plain image. When compared with another methods, the value of NPCR and UACI are competitive in Table 4.

Table 3. NPCR and UACI values for grayscale image

Grayscale Image	NPCR (%)	UACI (%)
Cameraman	99.60938	33.51582
Clock	99.55902	33.64326
Boats	99.58611	33.45125
Baboon	99.61624	33.39060

Table 4. NPCR and UACI values of Cameraman image compared to other method

Method	Proposed	[18]	[17]	[19]	[20]
NPCR (%)	99.60785	99.62769	99.6521	99.60481	99.5956
UACI (%)	33.31048	33.43764	33.4538	33.48555	33.4508

Key Sensitivity Analysis

The difference of secret keys value used to encrypt and decrypt is important to amplify the security of the algorithm. A reliable algorithm should demonstrate sensitivity to even a slight change in the secret keys which results an overall change in the cipher image. Figure 6 gives the cipher images of Cameraman with slight difference in the secret keys and the difference between the cipher image with the original secret keys and the cipher image with slight different secret keys.

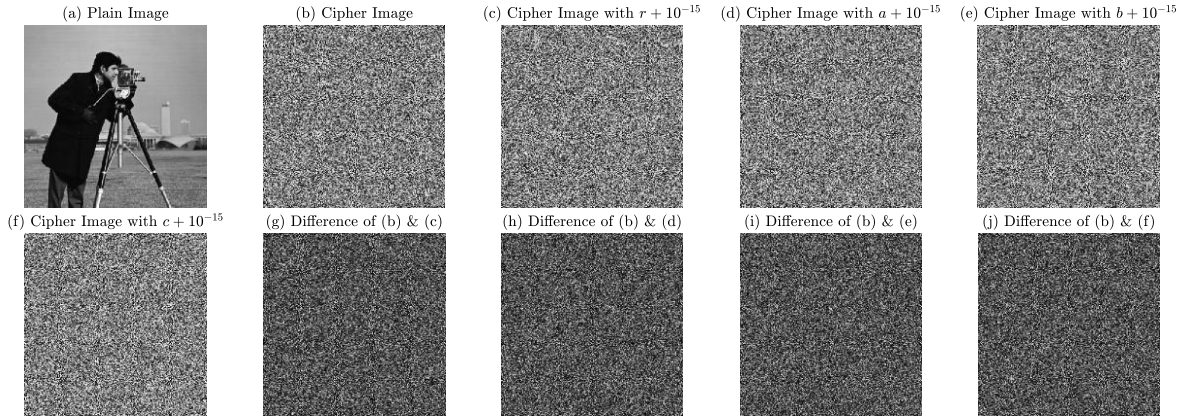

Figure 6. Key sensitivity analysis in encryption process

From Figure 6, we can see that with a slight change of the secret key value either r, a, b or c, the cipher image is entirely changed. This means that the proposed algorithm is sensitive to secret keys.

Histogram Analysis

A secure cipher image has a uniform pixel distribution. The uniform distribution of pixels in Cameraman image is displayed in Figure 7. With the intention of measuring the pixel distribution uniformness, one can use the Chi-square test with the following equation [27]

$$\chi^2 = \sum_{i=1}^{256} \frac{(M_i - m)^2}{m},$$

where M_i represents the frequency of pixel $i(i = 0,1,\ldots,255)$ and $m = \frac{M \times N}{256}$. The value of χ^2 needed for a histogram to be considered uniform with $\alpha = 0.05$ as the significance level is less than 293.2478. Table 5 indicates the values of χ^2 for almost all cipher images is below 293.2478. Therefore, the histogram is considered to be uniform. The value of χ^2 compared with other method is given in Table 6.

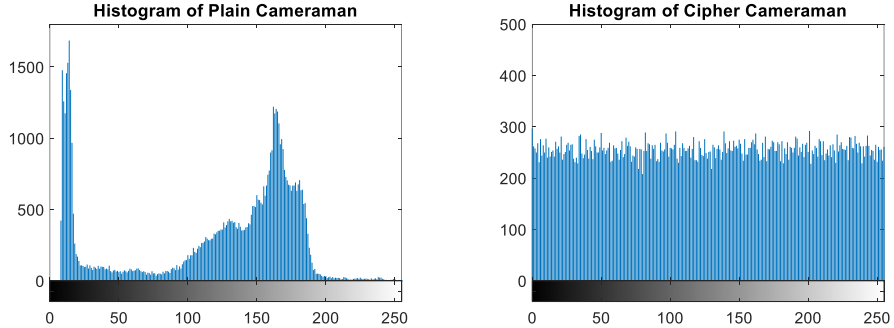

Figure 7. Histogram of plain and cipher image Cameraman

Table 5. χ^2 values of cipher grayscale images

Cipher Grayscale Image	PSNR
Cameraman	232.19531
Clock	220.22656
Boats	248.83398
Baboon	234.89258

Table 6. χ^2 values of Cameraman image compared with other methods

Method	Proposed	[8]	[19]	[20]	[22]
χ^2	278.72656	235.0123	269.0859	291.6484	278.72656

Mean Square Error (MSE) and Peak Signal-to-Noise Ratio Analysis (PSNR)

The quadratic error between plain image and cipher image is defined as follows

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{N} [PI^*(i,j) - CI^*(i,j)]^2$$

where $PI^*(i,j)$ and $CI^*(i,j)$ is the plain image and cipher image, respectively. Meanwhile, Peak Signal-To-Noise Ratio (PSNR) is defined in the following equation.

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\text{MSE}} \right).$$

MSE and PSNR can be utilized to evaluate the quality of cipher image. MSE should gives a high value, while PSNR should give a low value. The PSNR and MSE values for grayscale images are given in Table 7, while Table 8 gives the comparison with other literature. With the low PSNR and high MSE values, analysis result confirms that the cipher images have good quality.

Table 7. MSE and PSNR values of grayscale images

Grayscale Image	MSE	PSNR
Cameraman	9431.21869	8.38513
Clock	12242.71889	7.25202
Boats	7927.06595	9.13968
Baboon	6785.74157	9.81483

Table 8. MSE and PSNR values of Cameraman image compared with other methods

Method	Proposed	[8]	[19]	[20]	[21]	[22]
MSE	9431.64316	9520.0748	-	7796	9365.72411	10048.4797
PSNR	8.38493	8.3444	-	9.2118	8.41539	8.1098

Entropy

In 1948, Claude Shannon introduced the entropy concept [2]. The randomness of information can be evaluated using entropy. Entropy of a grayscale image is expressed by the following equation:

$$\text{En}(x) = -\sum_{i=0}^{255} p(x_i) \log_2 \big(p(x_i)\big).$$

where $p(x_i)$ denotes the probability associated with the occurrence of pixel value x_i. For grayscale image, the optimal value of entropy [2] is 8, which means the value of entropy of a cipher image should be nearly 8. Table 9 presented the entropy value for grayscale images and comparison with other methods. The values of the entropy are nearly 8, hence

the cipher image is random.

Table 9. Entropy values of cipher grayscale images and comparison with other methods

Grayscale Image	Methods					
	Proposed	**[7]**	**[19]**	**[20]**	**[21]**	**[22]**
Cameraman	7.99693	7.9972	7.99704	7.9968	7.99696	7.9993
Clock	7.99722	7.9970	7.99706	-	-	-
Boats	7.99928	-	7.99925	-	-	-
Baboon	7.99939	7.9969	7.99930	7.9976	7.99923	7.9992

Robustness Analysis

The decryption process can be evaluated its quality from a data change or loss with robustness analysis. For the data change test shown in Figure 8, the cipher image is added the speckle noise, gaussian noise and salt-and-pepper noise. Meanwhile, the cipher image is added the reduction of some pixels value for the data loss test shown in Figure 9. The outcome shows that the decrypted image from an encrypted image with noise or loss of data is still can be recognized. This shows that the presented decryption algorithm is resilient against noise and data loss.

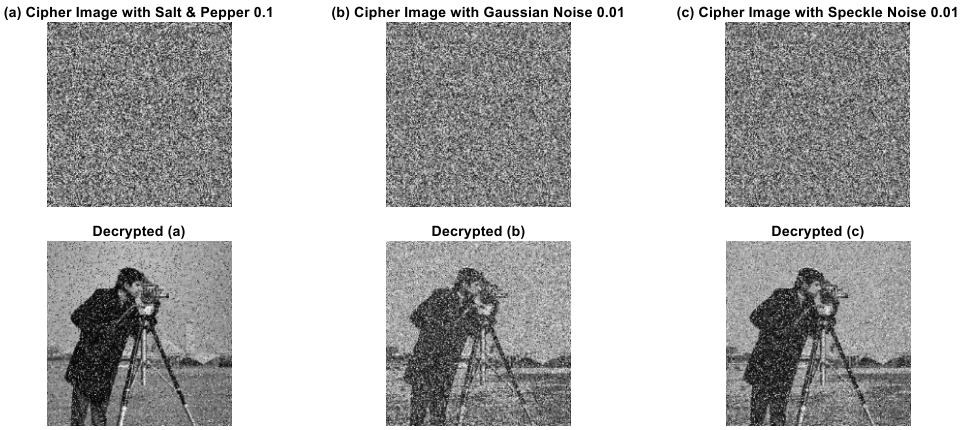

Figure 8. Data noise analysis for Cameraman image

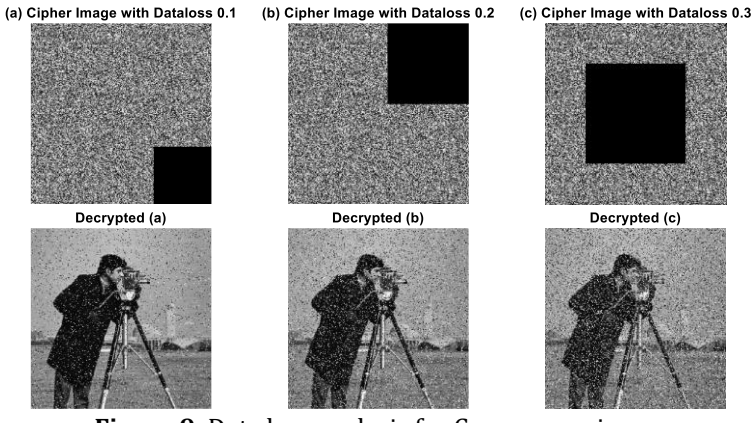

Figure 9. Data loss analysis for Cameraman image

Time Efficiency Analysis

A performance comparison was conducted between the proposed method and existing approaches in terms of encryption and decryption efficiency. As shown in Table 10, the proposed algorithm achieves encryption and decryption times of less than one

second, indicating its suitability for real-time communication applications. Moreover, Table 10 clearly demonstrates that the proposed method offers superior runtime performance compared to other literatures.

Table 10. Encryption and decryption time comparison for Cameraman image in second

Process	Proposed	[18]	[19]	[20]
Encryption Time	0.2562	0.6007	0.1888	3.319
Decryption Time	0.0573	0.3804	0.1838	-

CONCLUSIONS

This paper applies the logistic map with feedback control (LMFC), which is a chaotic map into an image encryption algorithm for grayscale and RGB image. Four control parameters of the map are used as secret keys to calculate the step size of the map which maximize the Lyapunov exponent and generate the pseudo-random sequence. A permutation process is done using the generated sequence from LMFC to scramble the position of the pixels. To encrypt further, bit-wise XOR operation between the pixels value and the keystream is used to diffuse the pixels value, resulting in a cipher image. It has been determined through performance analysis that the algorithm has a substantial key space, resilient to brute-force attacks and exceedingly sensitive to plain image and secret keys. Furthermore, the resulting cipher image shows an almost no correlation between its adjacent pixels, uniform histogram, high MSE and low PSNR value. Cipher image can be considered random as the entropy closely approach the optimal value. Decrypted image from cipher image with noise or data loss still can be recognized, indicates a good decryption algorithm quality.

REFERENCES

[1] F. E. Abd El-Samie, H.E.H Ahmed, I. F. Elashry, M. H. Shahieen, O. S. Faragallah E-S. M. El-Rabaie, and S. A. Alshebeili, "*Image encryption: a communication perspective*". CRC Press, 2013. DOI: 10.1201/b16309.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal,* vol. 28, no. 4, pp. 656-715, 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[3] Q. Zhang and Q. Ding, "Digital image encryption based on advanced encryption standard (AES)," in *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 2015, pp. 1218-1221: IEEE.

[4] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," Optik, vol. 261, p. 169122, 2022.

[5] K. Gopalsamy and P.-X. Weng, "Feedback regulation of logistic growth," *International Journal of Mathematics and Mathematical Sciences,* vol. 16, pp. 177-192, 1993. DOI: 10.1155/S0161171293000213.

[6] D.-y. WU, "Bifurcation analysis of a discrete Logistic system with feedback control," *Chinese Quarterly Journal of Mathematics,* vol. 30, no. 1, p. 66, 2015. DOI: 10.13371/j.cnki.chin.q.j.m.2015.01.008.

[7] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption," *Symmetry,* vol. 15, no. 5, p. 1081, 2023.

[8] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, no. 118253-70, 2021. DOI: 10.1109/ACCESS.2021.3106028.

[9] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences," *Entropy,* vol. 22, no. 2, p. 158, 2020. DOI: 10.3390/e22020158.

[10] A. A. Neamah and A. A. Shukur, "A Novel Conservative Chaotic System Involved in Hyperbolic Functions and Its Application to Design an Efficient Colour Image Encryption Scheme," *Symmetry,* vol. 15, no. 8, p. 1511, 2023. DOI: 10.3390/sym15081511.

[11] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Information Sciences,* vol. 515, pp. 191-217, 2020. DOI: 10.1016/j.ins.2019.10.070.

[12] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Logistic sine map based image encryption," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, 2019, pp. 290-295: IEEE.

[13] A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption," *Electronics,* vol. 10, no. 12, p. 1392, 2021.

[14] D. Herbadji, N. Derouiche, A. Belmeguenai, A. Herbadji, and S. Boumerdassi, "A tweakable image encryption algorithm using an improved logistic chaotic map," *Traitement du Signal,* vol. 36, no. 5, pp. 407-417, 2019. DOI: 10.18280/ts.360505.

[15] R. Li, Q. Liu, and L. Liu, "Novel image encryption algorithm based on improved logistic map," *IET Image Processing,* vol. 13, no. 1, pp. 125-134, 2019. DOI: 10.1049/iet-ipr.2018.5900.

[16] Q. Lu, L. Yu, and C. Zhu, "Symmetric image encryption algorithm based on a new product trigonometric chaotic map," *Symmetry,* vol. 14, no. 2, p. 373, 2022. DOI: 10.3390/sym14020373.

[17] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications,* vol. 78, pp. 22023-22043, 2019. DOI: 10.1007/s11042-019-7453-3.

[18] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image encryption scheme based on newly designed chaotic map and parallel DNA coding," *Mathematics,* vol. 11, no. 1, p. 231, 2023. DOI: 10.3390/math11010231.

[19] M. Demirtaş, "A novel multiple grayscale image encryption method based on 3D bit-scrambling and diffusion," *Optik,* vol. 266, p. 169624, 2022. DOI: 10.1016/j.ijleo.2022.169624.

[20] M. Akraam, T. Rashid, and S. Zafar, "A chaos-based image encryption scheme is proposed using multiple chaotic maps," *Mathematical Problems in Engineering,* vol. 2023, 2023. DOI: 10.1155/2023/2003724.

[21] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, A. Y. Al-Dubai, "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access,* vol. 10, pp. 12966-12982, 2022. DOI: 10.1109/ACCESS.2022.3146792.

[22] S. De, J. Bhaumik, and D. Giri, "A secure image encryption scheme based on three different chaotic maps," *Multimedia Tools and Applications,* vol. 81, no. 4, pp. 5485-5514, 2022.

[23] A. Pikovsky and A. Politi, *Lyapunov exponents: a tool to explore complex dynamics*. Cambridge University Press, 2016. DOI: 10.1017/CBO9781139343473.

[24] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing,* vol. 168, p. 107340, 2020. DOI: 10.1016/j.sigpro.2019.107340.

[25] J. Liu, D. Yang, H. Zhou, and S. Chen, "A digital image encryption algorithm based on bit-planes and an improved logistic map," *Multimedia Tools and Applications,* vol. 77, pp. 10217-10233, 2018. DOI: 10.1007/s11042-017-5406-2.

[26] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT),* vol. 1, no. 2, pp. 31-38, 2011.

[27] P. N. Andono, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access,* vol. 10, pp. 115143-115156, 2022. DOI: 10.1109/ACCESS.2022.3218886.